bind()

Race and conflict conditions with mulitple processes or threads attempting to bind to the same port and IP adress

Sean Barnum, Cigital, Inc. [vita[1]]

2005-10-03

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3468 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Denial of Service</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Race Condition</td></tr>
<tr><td><b>Software Context</b></td><td>• Networking</td></tr>
<tr><td><b>Location</b></td><td>• sys/socket.h</td></tr>
<tr><td><b>Description</b></td><td>bind() takes an unnamed socket and assigns a name to it. This name, in the case of a network socket, is an IP address and a port.
If two processes (or even two threads) want to bind to the same port at the same IP address, a race condition will exist and only one process will be allowed to have the port. The other call will return an error.
Also, if a server binds to a socket interface with a ‘vague’ address first (say, all IP addresses) and then another server binds with more specific address (say, 192.158.2.27, the IP of the box) then the second server will get the traffic. A Windows addition has been made to remedy this setsockopt(...SO_EXCLUSIVEADDRUSE,...)</td></tr>
<tr><td><b>APIs</b></td><td><table><tr><th>FunctionName</th><th>Comments</th></tr><tr><td>bind()</td><td></td></tr></table></td></tr>
<tr><td><b>Method of Attack</b></td><td>An attacker could write another program to open the same port on the same IP address that he or she knows the target program will. When the target program tries to do so, it will fail and access to the service it provides will be denied.
Bind can also be used maliciously</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr><tr><td>This solution is applicable</td><td>Bind to a port lower than</td><td>Binding to a port lower</td></tr></table></td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

<table>
<tr><td></td><td><table><tr><td>if the host is a running a Unix-based operating system and the process is being run with super-user privileges.</td><td>1024. Only processes run by the super-user have the ability to bind to these ports.</td><td>than 1024 will restrict which processes can compete for access to the same port on the same IP.</td></tr></table></td></tr>
<tr><td><b>SignatureDetails</b></td><td>int bind(int s, const struct sockaddr *name, socklen_t namelen);</td></tr>
<tr><td><b>Examples of Incorrect Code</b></td><td></td></tr>
<tr><td><b>Examples of Corrected Code</b></td><td></td></tr>
<tr><td><b>Source References</b></td><td><ul><li>ITS4 Source Code Vulnerability Scanning Tool [2]</li><li>bind() man page[3]</li><li>Howard, Michael & LeBlanc, David C. <i>Writing Secure Code</i>, 2nd ed. Redmond, WA: Microsoft Press, 2002, ISBN: 0735617228.</li></ul></td></tr>
<tr><td><b>Recommended Resources</b></td><td></td></tr>
<tr><td><b>Discriminant Set</b></td><td><table><tr><td><b>Operating System</b></td><td><ul><li>UNIX (All)</li></ul></td></tr><tr><td><b>Languages</b></td><td><ul><li>C</li><li>C++</li></ul></td></tr></table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com